APPENDIX A

Pending Claims 74-124 After Entering of Amendments

74. A method of authenticating a dispatch and contents of the dispatch transmitted from a sender to a recipient, comprising the steps of:

sending content data representative of the contents of the dispatch, and a destination of the dispatch associated with said recipient, to an authenticator functioning as a non-interested third party with respect to the sender and the recipient, to be forwarded to said destination;

receiving a representation of authentication data that has been generated by said authenticator, said authentication data comprising a representation of the following set A of information elements: a_1 - comprising said content data, and dispatch record data elements a_2,..., a_n which includes at least an indicia a_2 relating to a time of the dispatch which is provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and an indicia a_3 relating to said destination of the dispatch,

wherein at least part of said authentication data is secured against tampering of the sender and the recipient, and

wherein said authentication data includes a set B comprising one or more information elements b_1,..., b_m generated by respectively applying functions F_1, ..., F_m to subsets S_1, ..., S_m comprising selected portions of said set A, where said functions F_1, ..., F_m can be different from one another and said subsets S_1, ..., S_m can be different from one another, and

wherein said authentication data does not comprise an encrypted representation of said content data and said dispatch record data which is encrypted with a secret key, either symmetric or asymmetric, associated with said recipient.

75. Authentication data for authenticating a dispatch and contents of the dispatch electronically transmitted from or for a sender to a recipient, comprising a representation of the following set A of information elements:

content data a_1 representative of the contents of a dispatch; and

dispatch record data elements $a_2,..., a_n$ which include at least an indicia a_2 relating to a time of the dispatch and an indicia a_3 relating to the destination of the dispatch,

wherein said time related indicia a_2 being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and

wherein at least part of said authentication data is secured against tampering of the sender and the recipient, and

wherein said authentication data are generated and secured by an authenticator functioning as a non-interested third party with respect to the sender and the recipient, and

wherein said authentication data includes a set B comprising one or more information elements $b_1,..., b_m$ generated by respectively applying functions $F_1, ..., F_m$ to subsets $S_1, ..., S_m$ comprising selected portions of said set A, where said functions $F_1, ..., F_m$ can be different from one another and said subsets $S_1, ..., S_m$ can be different from one another, and

wherein said authentication data does not comprise an encrypted representation of said content data and said dispatch record data which is encrypted with a secret key, either symmetric or asymmetric, associated with said recipient.

76. A method for verifying the authenticity of a dispatch sent from a sender to a recipient, comprising the steps of:

providing a representation of a selected portion of a group A' of data elements purported authentic, said elements including a content data, and dispatch record data comprising at least a time and destination relating to the dispatch;

comparing said representation for match with a representation of at least part of authentication data, that has been generated by an authenticator functioning as a non-interested third party with respect to the sender and the recipient, said authentication data comprising a representation of the following set A of information elements: a_1 - comprising a content data, and dispatch record data elements a_2,..., a_n which includes at least an indicia a_2 relating to a time of the dispatch which is provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and an indicia a_3 relating to said destination of the dispatch,

wherein at least part of said authentication data is secured against tampering of the sender and the recipient, and

wherein said authentication data includes a set B comprising one or more information elements b_1,..., b_m generated by respectively applying functions F_1, ..., F_m to subsets S_1, ..., S_m comprising selected portions of said set A, where said functions F_1, ..., F_m can be different from one another and said subsets S_1, ..., S_m can be different from one another, and

wherein said authentication data does not comprise an encrypted representation of said content data a_1 and said dispatch record data elements a_2,..., a_n which is encrypted with a secret key, either symmetric or asymmetric, associated with said recipient.

77. A method according to claim 74 wherein said authenticator and said recipient do not share a secret key.

78. A method according to claim 74 wherein said securing of the authentication data is performed in a manner other than by encryption using a secret key associated with said recipient.

79. A method according to claim 74 wherein said authentication data is generated using no secret key associated with said recipient.

80. A method according to claim 74 wherein said authentication data possesses the property that encrypted information, if any, that it consists of is generated using no secret key associated with said recipient.

81. A method according to claim 74 wherein said dispatch record data comprises at least one element selected from the group consisting of a delivery indication associated with said dispatch, the number of pages transmitted, page numbers, an indication of identification associated with said sender, said dispatch duration, integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said authenticator, a heading message, a trailing message, and a link information element through which other selected elements of the authentication data or said set A are linked and associated to each other.

82. A method according to claim 81 wherein said delivery indication is generated using no secret key associated with said recipient.

83. A method according to claim 81 wherein said delivery indication comprises information returned by or associated with said recipient or an agent of said recipient.

84. A method according to claim 74 wherein said securing of the authentication data includes storing a selected portion thereof in secure storage.

85. A method according to claim 84 wherein said storage is associated with a third party, thereby rendering it secure.

86. A method according to claim 74 wherein said authenticator comprises at least one element of the group consisting of a facsimile machine, a modem, a network interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a message transmission forwarding service.

87. A method according to claim 74 or 83 wherein said dispatch is delivered to an agent of said recipient.

88. A method according to claim 74 wherein said element a_3 comprises at least one element of the group consisting of an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

89. A method according to claim 74 or 81 wherein at least one of said functions $F_1, \ldots, F_m$ is selected from the group consisting of functions from the Hiding Class, functions unknown to the sender, one-way functions, symmetric or asymmetric digital signature functions, reversible or irreversible functions, compound functions and combinations thereof.

90. A method according to claim 74 or 81 wherein said authentication data comprises an element generated according to a Time-Stamping or a digital signature scheme.

91. A method according to claim 81 wherein said link information element comprises a dispatch identifier.

92. A method according to claim 74 or 81 wherein said representation of the authentication data is in the form a paper printout, electronic information, microfiche, and combinations thereof.

93. A method according to claim 75 wherein said authenticator and said recipient do not share a secret key.

94. A method according to claim 75 wherein said securing of the authentication data is performed in a manner other than by encryption using a secret key associated with said recipient.

95. A method according to claim 75 wherein said authentication data is generated using no secret key associated with said recipient.

B

96. A method according to claim 75 wherein said authentication data possesses the property that encrypted information, if any, that it consists of is generated using no secret key associated with said recipient.

97. A method according to claim 75 wherein said dispatch record data comprises at least one element selected from the group consisting of a delivery indication associated with said dispatch, the number of pages transmitted, page numbers, an indication of identification associated with said sender, said dispatch duration, integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said authenticator, a heading message, a trailing message, and a link information element through which other selected elements of the authentication data or said set A are linked and associated to each other.

98. A method according to claim 97 wherein said delivery indication is generated using no secret key associated with said recipient.

99. A method according to claim 97 wherein said delivery indication comprises information returned by or associated with said recipient or an agent of said recipient.

100. A method according to claim 75 wherein said securing of the authentication data includes storing a selected portion thereof in secure storage.

101. A method according to claim 100 wherein said storage is associated with a third party, thereby rendering it secure.

102. A method according to claim 75 wherein said authenticator comprises at least one element of the group consisting of a facsimile machine, a modem, a network interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a message transmission forwarding service.

103. A method according to claim 75 or 99 wherein said dispatch is delivered to an agent of said recipient.

104. A method according to claim 75 wherein said element a_3 comprises at least one element of the group consisting of an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

105. A method according to claim 75 or 97 wherein at least one of said functions $F_1, \ldots, F_m$ is selected from the group consisting of functions from the Hiding Class, functions unknown to the sender, one-way functions, symmetric or asymmetric digital signature functions, reversible or irreversible functions, compound functions and combinations thereof.

106. A method according to claim 75 or 97 wherein said authentication data comprises an element generated according to a Time-Stamping or a digital signature scheme.

107. A method according to claim 97 wherein said link information element comprises a dispatch identifier.

108. A method according to claim 75 or 97 wherein said representation of the authentication data is in the form a paper printout, electronic information, microfiche, and combinations thereof.

109. A method according to claim 76 wherein said authenticator and said recipient do not share a secret key.

110. A method according to claim 76 wherein said securing of the authentication data is performed in a manner other than by encryption using a secret key associated with said recipient.

111. A method according to claim 76 wherein said authentication data is generated using no secret key associated with said recipient.

112. A method according to claim 76 wherein said authentication data possesses the property that encrypted information, if any, that it consists of is generated using no secret key associated with said recipient.

113. A method according to claim 76 wherein said dispatch record data comprises at least one element selected from the group consisting of a delivery indication associated with said dispatch, the number of pages transmitted, page numbers, an indication of identification associated with said sender, said dispatch duration, integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said authenticator, a heading message, a trailing message, and a link information element through which other selected elements of the authentication data or said set A are linked and associated to each other.

114. A method according to claim 113 wherein said delivery indication is generated using no secret key associated with said recipient.

115. A method according to claim 113 wherein said delivery indication comprises information returned by or associated with said recipient or an agent of said recipient.

116. A method according to claim 76 wherein said securing of the authentication data includes storing a selected portion thereof in secure storage.

117. A method according to claim 116 wherein said storage is associated with a third party, thereby rendering it secure.

118. A method according to claim 76 wherein said authenticator comprises at least one element of the group consisting of a facsimile machine, a modem, a network interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a message transmission forwarding service.

119. A method according to claim 76 or 115 wherein said dispatch is delivered to an agent of said recipient.

120. A method according to claim 76 wherein said element a_3 comprises at least one element of the group consisting of an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

121. A method according to claim 76 or 113 wherein at least one of said functions $F_1, \ldots, F_m$ is selected from the group consisting of functions from the Hiding Class, functions unknown to the sender, one-way functions, symmetric or asymmetric digital signature functions, reversible or irreversible functions, compound functions and combinations thereof.

122. A method according to claim 76 or 113 wherein said authentication data comprises an element generated according to a Time-Stamping or a digital signature scheme.

123. A method according to claim 113 wherein said link information element comprises a dispatch identifier.

124. A method according to claim 76 or 113 wherein said representation of the authentication data is in the form a paper printout, electronic information, microfiche, and combinations thereof.